REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested.

Claims 1-12 remain pending. New claims 13-19 have been added to secure an appropriate scope of protection to which applicant is believed entitled.

A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. Kim fails to anticipate the subject matter of claim 1 as Kim fails to disclose reading events representing various types of system calls. Kim is directed to a tool for monitoring a designated set of files and directories for any changes and not to reading events as in the claimed subject matter. Kim is "[u]sed with system files on a regular (e.g., daily) basis." Kim at Abstract. The Examiner's attention is directed to page 4, lines 7-10 of the present specification for a brief description of events, e.g., "'[e]vents' in this context are kernel audit records read from the IDDS subsystem." Events include kernel audit records, which pertain to system call invocations by a process. In contrast, Kim describes employing signature routines to identify changes in files without reading events as in the claimed subject matter. For at least this reason, claim 1 is patentably distinguishable from Kim and the rejection should be withdrawn.

Claims 2-6 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over Kim for at least the reasons advanced above with respect to claim 1. The rejection of claims 2-6 should be withdrawn.

Claim 7 is patentable over Kim for reasons similar to those advanced above with respect to claim 1. The rejection of claim 7 should be withdrawn.

Claims 8-12 depend from claim 7, include further important limitations, and are patentable over Kim for at least the reasons advanced above with respect to claim 7. The rejection of claims 8-12 should be withdrawn.

New claim 14 recites a system for detecting critical file changes, comprising a processor; and a memory storing instructions. When the instructions are executed by the processor, the processor: routes events to an appropriate template, wherein the event includes one or more parameters; filters the event as either a possible intrusion based on one of the one or more

parameters and either dropping the event or outputting the event; and creates an intrusion alert if an event is output from the filter.

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN & BERNER, LLP

Randy A. Noranbrock
Registration No. 42,940

Customer Number: 22429
1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: June 7, 2005
KMB/RAN/iyr